PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-056965
(43)Date of publication of application : 25.02.2000

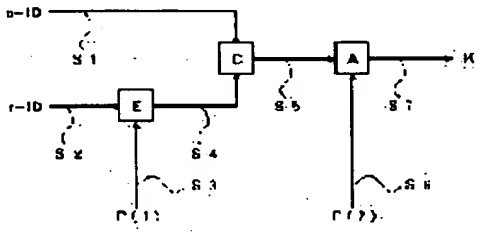
(51)Int.Cl. G06F 9/06
G06F 12/14

(21)Application number : 10-229879
(22)Date of filing : 17.08.1998

(71)Applicant : OKAMOTO TAKETOSHI
(72)Inventor : OKAMOTO TAKETOSHI

(54) DEVICE HAVING IDENTIFICATION INFORMATION, AND METHOD FOR USING IDENTIFICATION INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the identification information for device incapable of learning its contents by any person other than a software developing person in a software protection system using a password key.
SOLUTION: The device having irregular information issued for every device and information intrinsic to the device issued for every device is used, and the result obtained by composing the information extracted from irregular information issued for every device by the method decided by a software generator and the information intrinsic to the device issued for every device is used as the plain sentence for password key generation.



LEGAL STATUS

[Date of request for examination] 17.08.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－56965
（P2000－56965A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
G06F	9/06	550	G06F	9/06	550C	5B017
	12/14	320		12/14	320A	5B076

審査請求　未請求　請求項の数５　ＯＬ　（全４頁）

(21)出願番号　特願平10－229879

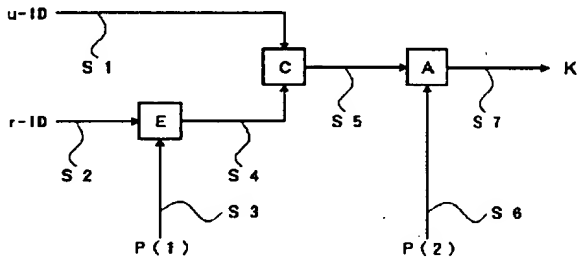
(22)出願日　平成10年８月17日(1998.8.17)

(71)出願人　594193313
岡本　健稔
岡山県倉敷市玉島1404番地
(72)発明者　岡本　健稔
岡山県倉敷市玉島乙島1809番地の３

Ｆターム(参考)　5B017 AA07 BA07 CA15
5B076 FA02 FB11

(54)【発明の名称】　識別情報を有する装置および識別情報の使用方法

(57)【要約】
【目的】　暗号キーを用いたソフトウェアプロテクトシステムにおいて、ソフトウェア開発者以外には、その内容を知ることができない装置の識別情報を提供する。
【構成】　装置ごとに発行される不規則な情報と、装置ごとに発行される装置に固有の情報を有する装置を用いて、装置ごとに発行される不規則な情報からソフトウェア作成者が決めた方法によって抽出した情報と、装置ごとに発行される装置に固有の情報を合成した結果を暗号キー生成の平文として使用する。



1

【特許請求の範囲】
【請求項１】　装置ごとに発行される不規則な情報と装置ごとに発行される固有の情報を有することを特徴とする装置。
【請求項２】　媒体ごとに発行される不規則な情報と媒体ごとに発行される固有の情報を記録した記録媒体。
【請求項３】　請求項１または請求項２の不規則な情報の一部と、請求項１または請求項２の固有の情報の全体または一部を使用することを特徴とする装置を識別する方法。
【請求項４】　請求項３の方法を用いたプログラムを記録した記録媒体。
【請求項５】　請求項３の方法を用いた手段を有する装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、コンピュータの装置を識別するための技術、主にソフトウェアの著作権保護に関するものである。
【０００２】
【従来の技術】コンピュータのソフトウェアは形のない無体物であるが、それを創りだすためには一般の利用者が想像もできないほどの、時間、費用、作成者の苦労と創造を必要とするものである。しかしながら、ソフトウェアの複写は、その投資に比べることもできないほどの短時間と少ない費用で簡単にできてしまう。このことはコンピュータを利用することの利点ではあるが、そうであるがゆえに使用料を支払わないでソフトウェアを使う、いわゆる違法コピーを蔓延させることにつながっている。違法コピーが大量に使われるとオリジナルの販売が少なくなり、作成者の投資を回収し利益を上げることが困難になり、よってオリジナルの使用料を高く設定することになり、違法コピーがさらに増えるという悪循環が起きる。このような現状は好ましくないことであり、適正な使用料をすべての利用者から回収する方法を確立する必要があることは、この業界の共通の認識である。
【０００３】そこで、従来から種々の対策、方法が考案されてきた。古くはコピーそのものを防止する方法。つまり、オリジナルの媒体からコピーしても使えない、または、コピー時にエラーが発生するような加工を施しておくものが使われた。いわゆるコピープロテクトである。しかし、この方法は、ソフトウェアのバックアップができない、プロテクトを破ってコピーするツールが販売されるなどの問題があり現在ではほとんど使われなくなった。
【０００４】最近、見られるプロテクトの方法として解除キーを用いた方法がある。これは、ソフトウェアの販売者が発行する解除キーを入力することで、暗号化して配布されたソフトウェアを復号化することができるもの、または、その使用に制限がかかっていたものが解除

2

できるものなどである。これらは、ソフトウェアのバックアップが可能であること、プロテクトを破ってコピーするツールに意味が無いことなどの特徴がある。
【０００５】前記の方法のうち制限の解除に解除キーを利用する方法として、特開平８－１２９４８６号公報にて開示されたものがある。この方法は、固有のコード（装置を識別するための装置に一意の情報）を有する装置において、その固有のコードを暗号化して「保護キー」を生成し、ソフトウェアに添付したキー情報と照合し、一致するならばソフトウェアを実行し、一致しないならば固有のコードを暗号化して「制限キー」を生成し、ソフトウェアの利用者に通知することで使用料の支払いを促し、ソフトウェアの販売者は、その「制限キー」を復号化し、「保護キー」を生成するのと同じ方法で「解除キー」を生成し利用者に通知する。利用者が「解除キー」を入力したならば「保護キー」と照合し、一致したならばソフトウェアに添付したキー情報を更新しソフトウェアを実行するものである。
【０００６】装置に固有のコードを暗号化する方法としては、剰余計算を用いるもの、転置と換字を併用するものなどがあるが、ここで問題となるのは、装置に固有のコードの内容（読み出し方法）を公開することが「暗号の強度」（悪用しようとする者が暗号化のアルゴリズムを解析することの困難さ）に影響するということである。
【０００７】
【発明が解決しようとする課題】装置の識別情報は広く一般に公開するものではないが、ソフトウェア開発者には、当然、それを公開しなければならない。しかし、このことは攻撃する者（プロテクトの方法を解析して悪用する者）にも知られてしまうことを意味している。つまり、攻撃する者は暗号化における平文（前記の固有のコード）と暗号文（前記の「制限キー」や「解除キー」など）の対を入手できると考えておく必要があり、また、広く情報を集めることで、その情報を自由に選択して攻撃（暗号化のアルゴリズムを解析して悪用）することができると考えられる。いかに暗号化のアルゴリズムと鍵（暗号化のパラメータ）が秘密であっても、いわゆる「選択平文攻撃」（攻撃する者が選択した平文に対する暗号文を入手することができるという攻撃側にとても有利な状況）にさらされることがわかっているとなれば、ソフトウェア開発者が安全性に不安を持つのも当然である。
【０００８】そこで、ソフトウェアの作成者以外には、暗号化の平文、つまり、装置の識別情報がどのような内容であるかを知ることができないようにする必要がある。
【０００９】
【課題を解決するための手段】本発明は、装置の識別情報として不規則な内容の情報を用い、かつ、ソフトウェ

アごとに決めた方法によってその情報の一部を抽出し用いることで、攻撃する者がその内容を知ることを困難にする。ただし、その情報のみを使用すると、異なる装置で情報が重複する可能性がある。そこで、装置に固有の情報を合わせて用いて重複を避けるのである。

【００１０】

【実施例】本発明の実施例について図１を参照して説明する。

【００１１】装置ごとに発行される不規則な情報ｒ－ＩＤをＳ２とし、任意の抽出パラメータＰ（１）であるＳ３を用いて抽出アルゴリズムＥにより、Ｓ２の一部を抽出した結果をＳ４とする。

【００１２】装置ごとに発行される不規則な情報ｒ－ＩＤの「不規則な」とは、たとえば、装置の製造番号のように順番になっている、もしくは、規則的な変化をしているようなものではないという意味である。つまり、０、１、２、３や０、２、４、８、１６のように並べることができるものではなく、できるならばランダムな内容を持つことが望ましい。しかし、それが純粋な乱数（特定の情報の出現率や連続発生率に偏りがなく、周期的な繰り返しがないもの）であることを必ずしも要求するものではない。

【００１３】不規則な情報の一部を抽出するとは次のような方法で識別情報の内容がわからないようにするものである。たとえば、０～９までの数値を各々１０個用意した１００桁の数値で、各桁の値をランダムに入れ換えたものを不規則な情報とし、その中の任意の桁位置で１０箇所の値をピックアップしたとき、任意の桁位置を知らないならば、その結果は、最小の「０００００００００」から最大の「９９９９９９９９９」までのどの値でもありえる。

【００１４】不規則な情報が、もし、装置の製造番号であり、その値が「０００００００００１」である装置と、「０００００００００２」である装置が存在すれば、その情報の一部を抽出したとしても、そのほとんどの桁の値は「０」であることが予測できる。「不規則な」の意味をさらに説明するならば、前記のように異なる装置で同じ値を持つ桁が多く存在することがない情報であり、それが装置に固有の情報であることは望ましい。

【００１５】複数の装置の識別情報を集めたとき、不規則な情報の中で偶然に値が一致する桁が多いとき、そのことを手がかりに攻撃することも考えられる。不規則な情報の桁数はなるべく多くすることが望ましい。たとえば、それが１０００桁程度の数値や文字情報であり、パソコンのＲＯＭに記録したとしても装置の設計や価格に影響を与えるようなものではないことは周知である。

【００１６】装置ごとに発行される固有の情報ｕ－ＩＤをＳ１とし、任意の合成手段ＣでＳ１とＳ４を合成した結果をＳ５とする。これが装置の識別情報である。装置

ごとに発行される固有の情報ｕ－ＩＤの中に、たとえば、将来使用するためのリザーブ領域や、日本国内で販売するときの国情報など識別しなくても問題ない部分があるならば、それを除外してＳ１としても問題ない。

【００１７】任意の合成手段Ｃは、Ｓ１とＳ４の各桁の値を交互に抽出し合成したり、Ｓ１とＳ４をつなげたものを任意のパラメータで転置するなど、適当な方法で合成する処理である。

【００１８】装置の識別情報Ｓ５を任意の暗号化アルゴリズムＡと暗号鍵Ｐ（２）であるＳ６で暗号化した結果Ｓ７が暗号キーＫである。これが、前記従来の技術で引用した「保護キー」や「制限キー」などである。

【００１９】つまり、前記従来の技術で引用した「固有のコード」に代わって、ソフトウェア開発者のみが、その内容を知り得る装置の識別情報Ｓ５を暗号化の平文として暗号化の処理に入力していることを理解していただきたい。

【００２０】装置の識別情報としてＳ４だけでなくＳ１を合成して使用する理由は、たとえば、Ｓ２の内容が「５３１４９１５９８２」の装置と、「５８９７９３２３８４」の装置があり、Ｓ３の指定が、１桁、５桁、９桁であるとすると、Ｓ４の値はどちらも「５９８」になり、当然、暗号キーＫも同じ内容になる。これを防止するため装置ごとに固有の情報Ｓ１を合成するのである。これにより、暗号キーＫは必ず装置ごとに異なる結果が得られる。

【００２１】装置ごとに発行される不規則な情報ｒ－ＩＤと、装置ごとに発行される固有の情報ｕ－ＩＤを装置に記録する請求項１の場合は、たとえば、パソコンの構成であれば、装置内の、ＲＯＭ、バッテリーバックアップされたＲＡＭ、マイクロプロセッサーの中、プリント板上の設定、ＬＡＮインターフェイスカードのアドレスＲＯＭ、ハードディスク等に記録する。ただし、ハードディスクに記録した場合は、イメージファイル作成・復元ツール、いわゆる、クローン作成ツールでコピーされると保護の意味がない。これを防止するためには、後記するようにＲＯＭやマイクロプロセッサーの中など、他の部品（ユニット）との併用が必要である。

【００２２】媒体に記録した識別情報を装置の読取部に装着し、その情報を読み取ることで装置の識別情報の代わりとして扱うことができる。つまり、媒体ごとに発行される不規則な情報ｒ－ＩＤと、媒体ごとに発行される固有の情報ｕ－ＩＤを記録媒体に記録する請求項２の場合は、識別情報をＩＣカードに記録し、それを装着した装置が、その識別情報を有する装置として動作するのである。

【００２３】このように、交換可能な媒体を用いると、ソフトウェアを使用したい装置にその媒体をセットして使用することが可能になる。たとえば、あるソフトウェアの使用料を支払った人が、自宅のパソコンと勤務先の

5

パソコンの両方でそのソフトウェアを使おうとしたとき、識別情報を記録した記録媒体を持ち歩くだけでどちらでも使うことができる。つまり、自宅用と勤務先用に２台分の使用料を支払わなくてよい、という利点が生まれる。

【００２４】識別情報を記録する記録媒体としては、複製を作ることが困難なＩＣカードを用いる。複製を作ることが簡単な磁気記録媒体や光ディスクなどを用いた場合は、その保護効果がないのは自明である。

【００２５】不規則な情報ｒ－ＩＤと、固有の情報ｕ－ＩＤを記録するとき、別の部品や媒体を用いることも可能である。たとえば、マイクロプロセッサーに固有の情報があり、不規則な情報を記録する設計がなされていなかったとしても、不規則な情報をハードディスクに記録することで運用が可能になる。クローン作成ツールでコピーしたとしても固有の情報が異なるため装置ごとに暗号キーは変化する。ただし、不規則な情報が同じ値である装置が多数存在すると、固有の情報の変化（差分）に対する暗号キーの変化の関係から暗号鍵を求める「差分攻撃法」を可能にするため、販売者側でチェックし警告をすることは必要である。

6

【００２６】

【発明の効果】以上説明したように本発明の装置、および、識別情報を使用する方法を用いれば、暗号キーを生成する元の平文（装置の識別情報）を特定することが困難になり、違法にソフトウェアを使用すること、および、暗号化のアルゴリズムを解析することを困難にすることができる。

【図面の簡単な説明】

【図１】本発明の実施例を示すブロック図である。

【符号の説明】

Ｓ１　装置ごとに発行される固有の情報ｕ－ＩＤ
Ｓ２　装置ごとに発行される不規則な情報ｒ－ＩＤ
Ｓ３　抽出パラメータＰ（１）
Ｓ４　不規則な情報ｒ－ＩＤから抽出した結果
Ｓ５　装置の識別情報
Ｓ６　暗号鍵Ｐ（２）
Ｓ７　暗号キーＫ
Ａ　　暗号化アルゴリズム
Ｃ　　合成アルゴリズム
Ｅ　　抽出アルゴリズム

【図１】